Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (canceled)

2. (canceled)

3. (canceled)

4. (canceled)

5. (canceled)

6. (canceled)

7. (currently amended) A computer implemented method for encrypting ~~a data element~~ and decrypting ~~said data element~~ using a first~~static~~ key and a second~~dynamic~~ key, comprising:

encrypting said data element with said first~~static~~ key and a current encryption state to produce a first encrypted data and an updated ~~, wherein said encrypting maintains an~~ encryption state;

encrypting said first encrypted data with said second key to produce a second encrypted data;

transmitting said second encrypted data with said current encryption state to a receiving computer system;

encrypting a subsequent data element with said first key and said updated encryption state to produce a subsequent first encrypted data and a subsequent updated encryption state;

encrypting said subsequent first encrypted data ~~element~~ with said second~~dynamic~~ key to produce a subsequent second encrypted data;

transmitting said subsequent second encrypted data ~~element~~ with said updated encryption state to a receiving computer system;

~~decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;~~

~~determining whether transmission of a previous encrypted data element failed; and~~

~~in response to said determining said transmission of said previous encrypted data element failed,~~

decrypting, on said receiving computer system, said subsequent second encrypted data ~~element~~ with said second key to produce a decrypted subsequent second encrypted data; and

decrypting said decrypted subsequent second encrypted data with said first~~static~~ key and[[,]] said updated encryption state transmitted with said subsequent second encrypted data ~~element~~ to produce a decrypted subsequent data element~~, and said dynamic key without retransmission of said previous encrypted data element~~.

8. (currently amended) The method of Claim 7, wherein said encrypting said data element with said first~~static~~ key strongly encrypts said data element with said first~~static~~ key; and wherein said encrypting said subsequent data element with said first key strongly encrypts said subsequent data element with said first key.

9. (currently amended) The method of Claim 7, wherein said encrypting said first encrypted data ~~element~~ with said second~~dynamic~~ key weakly encrypts said first encrypted data ~~element~~ with said second~~dynamic~~ key; wherein said encrypting said subsequent first encrypted data with said second key weakly encrypts said subsequent first encrypted data with said second key.

10. (currently amended) The method of Claim 7, ~~further comprising:~~

wherein said encrypting said data element with said first~~static~~ key is on a first computer system;

wherein said encrypting said subsequent data element with said first key is on said first computer system;

further comprising: transmitting said first encrypted data and said current encryption state from said first computer system ~~element~~ to a second computer system; and transmitting said subsequent first encrypted data and said updated encryption state from said first computer system to said second computer system;

wherein said encrypting said first encrypted data ~~element~~ with said second~~dynamic~~ key is on said second computer system.

wherein said encrypting said subsequent first encrypted data with said second key is on said second computer system, said second computer system being untrusted; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

11. (currently amended) The method of Claim 7,

wherein said encrypting said data element with said first~~static~~ key is on a first computer system;

wherein said encrypting said subsequent data element with said first key is on said first computer system;

wherein said encrypting said first encrypted data ~~element~~ with said second~~dynamic~~ key is on said first computer system;

wherein said encrypting said subsequent first encrypted data with said second key is on said first computer system; and

thereby distributing encryption and decryption between said first computer system and said receiving computer system.

12. (canceled)

13. (canceled)

14. (canceled)

15. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt ~~a data element~~ and decrypt ~~said data element~~ using a first~~static~~ key and a second~~dynamic~~ key, comprising:

encrypting ~~said~~ a data element with said first~~static~~ key and a current encryption state to produce a first encrypted data and an updated encryption state~~, wherein said encrypting maintains an encryption state~~;

encrypting said first encrypted data ~~element~~ with said second~~dynamic~~ key to produce a second encrypted data;

transmitting said second encrypted data ~~element~~ with said current encryption state to a receiving computer system;

encrypting a subsequent data element with said first key and said updated encryption state to produce a subsequent first encrypted data and a subsequent updated encryption state;

encrypting said subsequent first encrypted data with said second key to produce a subsequent second encrypted data;

transmitting said subsequent second encrypted data with said updated encryption state to said receiving computer system;

~~decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;~~

~~determining whether transmission of a previous encrypted data element failed; and~~

~~in response to said determining said transmission of said previous encrypted data element failed,~~

decrypting, on said receiving computer system, said subsequent second encrypted data ~~element~~ with said second key to produce a decrypted subsequent second encrypted data; and

decrypting said decrypted subsequent second encrypted data with said first ~~static~~ key and[[,]] said updated encryption state transmitted with said subsequent second encrypted data ~~element~~ to produce a decrypted subsequent data element~~, and said dynamic key without retransmission of said previous encrypted data element~~.

16. (currently amended) The article of manufacture of Claim 15 wherein said encrypting said data element with said first ~~static~~ key strongly encrypts said data element with said first ~~static~~ key, wherein said encrypting said subsequent data element with said first key strongly encrypts said subsequent data element with said first key.

17. (currently amended) The article of manufacture of Claim 15 wherein said encrypting said first encrypted data ~~element~~ with said second~~dynamic~~ key weakly encrypts said first encrypted data ~~element~~ with said second~~dynamic~~ key; and wherein said encrypting said subsequent first encrypted data with said second key weakly encrypts said subsequent first encrypted data with said second key.

18. (currently amended) The article of manufacture of Claim 15, ~~further comprising~~:

wherein said encrypting said data element with said first ~~static~~ key is on a first computer system;

wherein said encrypting said subsequent data element with said first key is on said first computer system;

further comprising:

transmitting said first encrypted data ~~element~~ and said current encryption state from said first computer system to a second computer system; and

transmitting said subsequent first encrypted data and said updated encryption state from said first computer system to said second computer system;

wherein said encrypting said first encrypted data ~~element~~ with said second ~~dynamic~~ key is on said second computer system, said second computer system being untrusted;

wherein said encrypting said subsequent first encrypted data with said second key is on said second computer system; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

19. (currently amended) The article of manufacture of Claim 15,

wherein said encrypting said data element with said first ~~static~~ key is on a first computer system;

wherein said encrypting said first encrypted data ~~element~~ with said second ~~dynamic~~ key is on said first computer system;

wherein said encrypting said subsequent data element with said first key is on said first computer system;

wherein said encrypting said subsequent first encrypted data with said second key is on said first computer system; and

thereby distributing encryption and decryption between said first computer system and said receiving computer system.

20. (canceled)

21. (canceled)

22. (canceled)

23. (canceled)

24. (canceled)

25. (canceled)

26. (canceled)

27. (canceled)

28. (canceled)

29. (currently amended) A computer implemented method for encrypting ~~a data element~~ and decrypting ~~said data element~~ using a first ~~static~~ key and a second ~~dynamic~~ key, wherein a ~~said~~ data element is ~~being~~ partitioned into chunks, comprising:

___encrypting ~~said~~ a data element chunk ~~chunks~~ with said first ~~static~~ key and a current encryption state to provide ~~static~~ a first encrypted chunk data and an updated encryption state;

___encrypting a subsequent data element chunk with said first key and said updated encryption state to provide a subsequent first encrypted chunk data and a subsequent updated encryption state~~data element chunks, said static encrypted data element chunks being associated with static encryption states, respectively said static encryption states being used to vary values of said static encrypted data element chunks being statically encrypted with said static key~~;

___encrypting said ~~static~~ first encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key to provide ~~dynamic-static~~ second encrypted chunk data ~~element chunks, respectively~~;

___transmitting said ~~dynamic-static~~ second encrypted chunk data ~~element chunks~~ and said ~~static~~ current encryption state ~~states~~ to a receiving computer system;

___encrypting said subsequent first encrypted chunk data with said second key to provide subsequent second encrypted chunk data;

transmitting said subsequent second encrypted chunk data and said updated encryption state to said receiving computer system;

~~decrypting said dynamic-static data element chunks with said static key and said dynamic key on said receiving computer system;~~

~~determining, on said receiving computer system, whether transmission of a previous one of said dynamic-static data element chunks failed; and~~

~~in response to said determining said transmission of said previous one of said dynamic-static data element chunks failed,~~

decrypting said ~~a~~ subsequent second encrypted chunk data with said second key~~one of said dynamic-static data element chunks~~; and

decrypting said decrypted subsequent second encrypted chunk data with said first ~~static~~ key and said updated encryption state~~, said dynamic key and one of said static encryption states~~ that is transmitted with said subsequent second encrypted chunk data to provide a decrypted subsequent data element chunk~~one of said dynamic-static data element chunks, wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not recovered~~.

30. (currently amended) The method of Claim 29 wherein said encrypting said data element chunk ~~chunks~~ with said first ~~static~~ key strongly encrypts said data element chunk ~~chunks~~ with said first ~~static~~ key, and wherein said encrypting said subsequent data element chunk with said first key strongly encrypts said subsequent data element chunk with said first key.

31. (currently amended) The method of Claim 29 wherein said encrypting said ~~static~~ first encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key weakly encrypts said first encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key, and wherein said encrypting said subsequent first encrypted chunk data with said second key weakly encrypts said subsequent encrypted chunk data with said second key.

32. (currently amended) The method of Claim 29, ~~further comprising:~~

wherein said encrypting said data element chunk ~~chunks~~ with said first ~~static~~ key is on a first computer system;

wherein said encrypting said subsequent data element chunk with said first key is on said first computer system;

further comprising:

transmitting said first ~~static~~ encrypted chunk data and said current encryption state ~~element chunks~~ to a second computer system; and

transmitting said subsequent first encrypted chunk data and said updated encryption state to said second computer system;

wherein said encrypting said ~~static~~ first encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key is on said second computer system,

wherein said encrypting said subsequent first encrypted chunk data with said second key is on said second computer system, second computer system being untrusted; and

thereby distributing encryption between said first computer system and said second computer system.

33. (currently amended) The method of Claim 29,

wherein said encrypting said data element chunk ~~chunks~~ with said ~~static~~ first key is on a first computer system;

wherein said encrypting said subsequent data element chunk with said first key is on said first computer system;

wherein said encrypting said ~~static~~ second encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key is on said first computer system;

wherein said encrypting said subsequent second encrypted chunk data with said second key is on said first computer system.

34. (currently amended) The method of Claim 29, further comprising:

determining, on said receiving computer system, whether a transmission failure of said second encrypted chunk data occurred; wherein in response to said transmission failure said second encrypted chunk data ~~previous one of said dynamic-static data element chunks~~ associated with said failed transmission is not retransmitted~~in response to said determining said transmission of said previous one of said dynamic-static data element chunks failed~~.

35. (canceled)

36. (canceled)

37. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt ~~a data element~~ and decrypt ~~said data element~~ using a first ~~static~~ key and a second~~dynamic~~ key, wherein a ~~said~~ data element is ~~being~~ partitioned into chunks, comprising:

encrypting ~~said~~ a data element chunk~~chunks~~ with said first ~~static~~ key and a current encryption state to produce a first encrypted chunk data and an updated encryption state~~, wherein said encrypting maintains an encryption state~~;

encrypting a subsequent data element chunk with said first key and said updated encryption state to produce a subsequent first encrypted chunk data and a subsequent updated encryption state;

encrypting said second encrypted chunk data ~~element chunks~~ with said second~~dynamic~~ key to produce a second encrypted chunk data;

encrypting said subsequent second encrypted chunk data with said second key to produce a subsequent second encrypted chunk data;

transmitting said second encrypted chunk data ~~element chunks~~ with said current encryption state to a receiving computer system;

transmitting said subsequent encrypted chunk data with said updated encryption state to said receiving computer system;

~~decrypting said data element chunks with said static key and said dynamic key on said receiving computer system;~~

~~determining whether transmission of said data element chunks from said second computer system to said receiving computer system failed; and~~

~~in response to said determining said transmission of said one of said dynamic-static data element chunks failed,~~

decrypting said~~a~~ subsequent second encrypted chunk ~~one of said~~ data ~~element chunks~~ with said second~~static~~ key; and

decrypting said decrypted subsequent second encrypted chunk data with said first key and [[,]] said updated encryption state that is transmitted with said subsequent second encrypted chunk data~~one of said data element chunks, and said dynamic key without retransmission of said one of said dynamic static data element chunks associated with said failed transmission~~.

38. (currently amended) The article of manufacture of Claim 37 wherein said encrypting said data element chunk~~chunks~~ said first~~static~~ key weakly encrypts said data element chunk~~chunks~~ with said first~~static~~ key, wherein said encrypting said subsequent data element chunk with said first key weakly encrypts said subsequent data element chunk with said first key.

39. (currently amended) The article of manufacture of Claim 37 wherein said encrypting said data element chunk~~chunks~~ with said second ~~dynamic~~ key weakly encrypts said data element chunk~~chunks~~ with said second ~~dynamic~~ key, wherein said encrypting said subsequent data element chunk with said second key weakly encrypts said subsequent data element chunk with said second key.

40. (currently amended) The article of manufacture of Claim 37, ~~further comprising:~~
wherein said encrypting said data element chunk~~chunks~~ with said first~~static~~ key is on a first computer system;
wherein said encrypting said subsequent data element chunk with said first key is on said first computer system;
further comprising:
transmitting said first encrypted chunk data ~~element chunks~~ to a second computer system;
transmitting said subsequent first encrypted chunk data to said second computer system;
wherein said encrypting said first encrypted chunk data ~~element chunks~~ with said second ~~dynamic~~ key is on said second computer system, said second computer system being untrusted;
wherein said encrypting said subsequent first encrypted chunk data with said second key is on said second computer system; and
thereby distributing encryption between said first computer system and said second computer system.

41. (currently amended) The article of manufacture of Claim 37,

wherein said encrypting said data element chunk~~chunks~~ with said first~~static~~ key is on a first computer system;

wherein said encrypting said subsequent data element chunk with said first key is on said first computer system;

wherein said encrypting said first encrypted chunk data ~~element chunks~~ with said second~~dynamic~~ key is on said first computer system; and

wherein said encrypting said subsequent first encrypted chunk data with said second key is on said first computer system.

42. (currently amended) The article of manufacture of Claim 40, further comprising:

determining when transmission of said second encrypted chunk data ~~element chunks~~ from said first computer system to said second computer system failed; and

in response to said determining, performing, on said first computer system, said decrypting said subsequent second encrypted chunk data and said decrypting said decrypted subsequent second encrypted chunk data thereby recovering said decrypting ~~of said data element chunks~~ without retransmission of said second encrypted chunk data.

43. (canceled)

44. (canceled)

45. (canceled)

46. (original) The method of Claim 7 wherein said data element comprises digital data representing audio and video information.

47. (original) The article of manufacture of Claim 15 wherein said data element comprises digital data representing audio and video information.

48. (currently amended) The method of Claim 7, wherein said transmitting said second encrypted data transmits a packet comprising said second encrypted data ~~element~~ with said current encryption state to said receiving computer system;

wherein said transmitting said subsequent second encrypted data transmits a subsequent packet comprising said subsequent second encrypted data with said updated encrypted state to said receiving computer system; and

further comprising: ~~wherein said~~

determining, on said receiving computer system, ~~determines~~ whether a transmission failure occurred ~~of said previous encrypted data element failed~~ based on identifying a loss of said ~~a previous~~ packet comprising said ~~previous~~ second encrypted data;

in response to said determining, performing said decrypting, on said receiving computer system, said subsequent second encrypted data; and said decrypting, on said receiving computer system, said decrypted subsequent second encrypted data~~element~~.

49. (currently amended) The article of manufacture of Claim 15, wherein said transmitting said second encrypted data transmits a packet comprising said second encrypted data ~~element~~ with said current encryption state to said receiving computer system;

wherein said transmitting said subsequent second encrypted data transmits a subsequent packet comprising said subsequent second encrypted data with said updated encryption state to said receiving computer system; and

further comprising:

~~wherein said~~ determining, on said receiving computer system, ~~determines~~ whether a transmission failure occurred ~~of said previous encrypted data element failed~~ based on identifying a loss of said ~~a previous~~ packet comprising said ~~previous~~ second encrypted data;

in response to said determining, performing said decrypting, on said receiving computer system, said subsequent second encrypted data; and said decrypting, on said receiving computer system, said decrypted subsequent second encrypted data~~element~~.

50. (New): The method of claim 7 further comprising:

determining, on said receiving computer system, whether transmission of said second encrypted data failed;

performing, on said receiving computer system, in response to said determining, said decrypting said subsequent second encrypted data with said second key, and said decrypting said decrypted subsequent second encrypted data with said first key and said updated encryption state transmitted with said subsequent second encrypted data.

51. (New): The method of claim 50 wherein said second encrypted data of said failed transmission is not retransmitted.

52. (New): The method of claim 50 wherein said second encrypted data of said failed transmission is not recovered.

53. (New): The method of claim 50 wherein said second encrypted data of said failed transmission is corrupt.

54. (new) A computer implemented method for encrypting and decrypting using a first key and a second key, comprising:

encrypting a data element with said first key to produce a first encrypted data;

encrypting said first encrypted data with said second key and a current encryption state to produce a second encrypted data and an updated encryption state;

transmitting said second encrypted data with said current encryption state to a receiving computer system;

encrypting a subsequent data element with said first key to produce a subsequent first encrypted data;

encrypting said subsequent first encrypted data with said second key and said updated encryption state to produce a subsequent second encrypted data and another updated encryption state;

transmitting said subsequent second encrypted data with said updated encryption state to a receiving computer system;

decrypting, on said receiving computer system, said subsequent second encrypted data with said second key and said updated encryption state that is transmitted with said second encrypted data; and

decrypting, on said receiving computer system, said decrypted subsequent second encrypted data with said first key.

55. (new) The method of Claim 54,

wherein said encrypting said data element with said first key to produce said first encrypted data is also based on a first-encryption encryption state to produce said first encrypted data and an updated first-encryption encryption state;

wherein said transmitting said second encrypted data with said current encryption state also transmits said first-encryption encryption state;

wherein said encrypting said subsequent data element with said first key to produce said subsequent first encrypted data is also based on said updated first-encryption encryption state to produce said subsequent first encrypted data and an updated subsequent first-encryption encryption state;

wherein said transmitting said subsequent second encrypted data with said updated encryption state also transmits said updated first-encryption encryption state; and

wherein, on said receiving computer system said decrypting said decrypted subsequent second encrypted data with said first key is also based on said updated first-encryption encryption state that is transmitted with said subsequent second encrypted data to produce said decrypted subsequent data element.

56. (new) The method of Claim 54,

wherein said encrypting said data element with said first key is on a first computer system;

wherein said encrypting said subsequent data element with said first key is on said first computer system;

further comprising: transmitting said first encrypted data with said current encryption state and said subsequent first encrypted data with said updated encryption state from said first computer system to a second computer system;

wherein said encrypting said first encrypted data with said second key is on said second computer system, wherein said encrypting said subsequent first encrypted data is on said second computer system, said second computer system being untrusted; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

57. (New): The method of claim 54 further comprising:

determining, on said receiving computer system, whether transmission of said second encrypted data failed; and

performing on said receiving computer system, in response to said determining, said decrypting said subsequent second encrypted data with said second key and said updated encryption state transmitted with said subsequent second encrypted data; and said decrypting said decrypted subsequent second encrypted data with said first key.

58. (New): The method of claim 57 wherein said second encrypted data of said failed transmission is not retransmitted.

59. (New): The method of claim 57 wherein said second encrypted data of said failed transmission is not recovered.

60. (New) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt and decrypt using a first key and a second key, comprising:

encrypting a data element with said first key to produce a first encrypted data;

encrypting said first encrypted data with said second key and a current encryption state to produce a second encrypted data and an updated encryption state;

transmitting said second encrypted data with said current encryption state to a receiving computer system;

encrypting a subsequent data element with said first key to produce a subsequent first encrypted data;

encrypting said subsequent first encrypted data with said second key and said updated encryption state to produce a subsequent second encrypted data and another updated encryption state;

transmitting said subsequent second encrypted data with said updated encryption state to a receiving computer system;

decrypting, on said receiving computer system, said subsequent second encrypted data with said second key and said updated encryption state that is transmitted with said second encrypted data; and

decrypting, on said receiving computer system, said decrypted subsequent second encrypted data with said first key.

61. (new) The article of manufacture of Claim 60

wherein said encrypting said data element with said first key to produce said first encrypted data is also based on a current first-encryption encryption state to produce said first encrypted data and an updated first-encryption encryption state;

wherein said transmitting said second encrypted data with said current encryption state also transmits said current first-encryption encryption state;

wherein said encrypting said subsequent data element with said first key to produce said subsequent first encrypted data is also based on said updated first-encryption encryption state to produce said subsequent first encrypted data and a subsequent updated first-encryption encryption state;

wherein said transmitting said subsequent second encrypted data with said updated encryption state also transmits said updated first-encryption encryption state; and

wherein, on said receiving computer system said decrypting said decrypted subsequent second encrypted data with said first key is also based on said updated first-encryption encryption state that is transmitted with said subsequent second encrypted data to produce said decrypted subsequent data element.

62. (new) The article of manufacture of Claim 60,

wherein said encrypting said data element with said first key is on a first computer system;

wherein said encrypting said subsequent data element with said first key and said current encryption state is on said first computer system;

further comprising:

transmitting said first encrypted data from a first computer system to a second computer system; and

transmitting said subsequent first encrypted data from said first computer system to said second computer system;

wherein said encrypting said first encrypted data with said second key is on said second computer system, said second computer system being untrusted; and

wherein said encrypting said subsequent first encrypted data with said second key is on said second computer system; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

63. (New): The article of manufacture of claim 60 further comprising:

determining, on said receiving computer system, whether transmission of said second encrypted data failed; and

in response to said determining, performing on said receiving computer system, said decrypting said subsequent second encrypted data with said second key and said updated encryption state transmitted with said subsequent second encrypted data, and said decrypting said decrypted subsequent second encrypted data with said first key.

64. (New): The article of manufacture of claim 63 wherein said second encrypted data of said failed transmission is not retransmitted.

65. (New): The article of manufacture of claim 63 wherein said second encrypted data of said failed transmission is not recovered.